TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

D2d Communication Security Lightweight Cryptographic Approach: Critical Survey

Ajith Kumar V[1], K Satyanarayan Reddy[2]
[1,]Research Scholar, Department of Computer Applications, Regional Research Center, VTU Belguam, India
[2]Professor Department of ISE,CAMBRIDGE INSTITUTE OF TECHNOLOGY (affiliated to VTU Belgaum),Bangalore

Article Info
Volume 82
Page Number: 5419 - 5432
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 27 January 2020*

Abstract:
Outgrowth of wireless mobile communication lead to new revolution. Smart phones are making inroads into socio-economic realms. Today we use smart phones almost like a personal computer. Some important milestones have been witnessed, such as number of fixed line Telephone connection has been surpassed by number of mobile phone connection, Number of connected/IP enabled devices in home surpassed more than one per person. In nutshell, people are living in a connected world, trying to connect unconnected things. Devices are becoming intelligent, smart and connected. Need for Device to Device communication is growing every day. D2D communication is becoming popular in health care, disaster or emergency services, power grid and lot many. Security cannot be undermined as D2D communication is becoming pivotal and impacting larger part of our life. In this paper our focus is on security challenges in D2D communication and explore remediation with lightweight cryptography. In this paper an effort has been made to study various techniques for securing D2D communication. This paper focuses on securing D2D communication using lightweight cryptography algorithms.

Keywords: *D2D Communication, Federal Information Processing Standard, Lightweight Cryptography, National Institute of Standards and Technology, User Equipment*

I. INTRODUCTION

Device to Device (D2D) communication is considered as one of the leading research areas. Communication in mobile network can be achieved by having one to one connection between two mobile users, without involving Base Station(BS) or backbone network. D2D communication in recent years crated lot of interest in Academia and Industry, surveys have been conducted by researchers exploring various possibilities of using D2D communication, such as disaster recovery, emergency services. Our contributions in this paper can be summarized as review of various literature on securing D2D communication, analyzing the key parameters identified by the research community for ensuring security such as privacy, secrecy, availability. Security requirements for various D2D scenarios such as full coverage, partial coverage and out of coverage conditions. Majority of the current work focuses on authentication, authorization of the end users and devices using traditional cryptography techniques, however we are looking at providing security for the data in transit. We strongly believe that there is a scope for using lightweight cryptography techniques to enhance security and increase the performance. This paper is organized as follows. Introduction, Section 2 focuses on classification of D2D communication, Section 3 deals with security requirements of D2D communication, here elaborate discussion is made on security requirements, various attack scenarios been identified. Section 4 covers the various works that has been carried out for ensuring security in D2D communication with a focus on

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

lightweight cryptography techniques. Section 5 conclude with identified research areas.

II. EVOLUTION OF D2D COMMUNICATION

D2D communication uses wireless mode and comparable to Mobile Ad-hock Networks (MANETS). Fig.1 shows the classification of Device to Device communication. Based on the recent academic and research developments D2D communication can be broadly classified into Inband D2D communication and Outband D2D communication.

Inband D2D communication further classified into Underlay andOverlay. in case of Underlay D2D communication, which uses same radio resources for cellular communication and D2D communication,D2D User Equipments compete with Cellular Users Equipments resulting in efficient use of resources, however, in this case there are some issues like interference and resource allocation. Researchers working in this area have proposed various algorithms for resolving interference issues, where as in case of Overlay communication, it uses dedicated radio resources , that is a certain portion of the band is reserved for D2D communication, thus avoiding contentions for the resources.

Outband D2D communication does not use the same wireless channel for D2D, instead uses Wi-Fi Direct/Blue tooth/Zigbee. In this research work, our focus is Outband D2D communication, hence D2D nodes should have 2 radio links one for Wireless and another for D2D communication using Wi-Fi Direct/Bluetooth/Zig-bee etc.

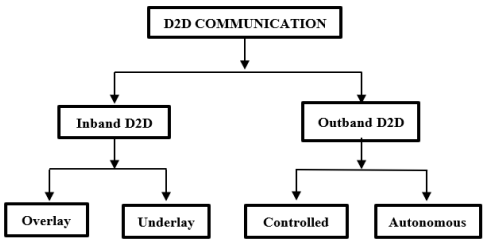

Figure 1. Device to Device Communication Classification [1]

Outband D2D communication can be further classified into Controlled D2D communication, where Service Provider controlled the second link, in case of Outband Autonomous D2D communication second link which is used for D2D communication is controlled by end user not by the service provider. There are some challenges and advantages in D2D communication. Advantages are offloading the communication from the centralized entity, saving the spectrum and bandwidth. Short range communications are typically characterized by higher throughput, lower delay and energy consumption when compared to long range communications.D2D communication can find applications in three scenarios.

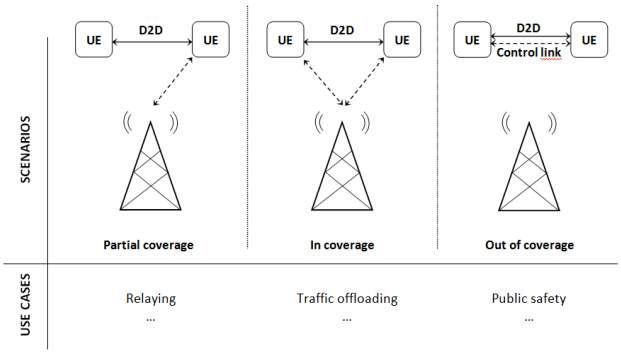

Figure 2. Uses cases of D2D Communication[18]

2.1. Full coverage

In coverage or full coverage where User Equipment (UEs) depends on the infrastructure facilities provided by the service provider. In many cases service provider facilities functions like device discovery, authentication, spectrum allocation and service provider generate revenue from this. This is synonym with normal communication in cellular networks, spectrum used for the communication is licensed spectrum.

Partial coverage

Partial coverage, in this scenario one of the UEs is facilitating D2D communication, by relaying cellular communication. This is typical use case of extending the coverage.

Out of coverage

Out of coverage, this is typical scenario where UEs are outside the coverage of service

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

provider cellular network and they directly communicate each other without using any of the service provider resources.

D2D communication opens new opportunities, this enables amalgamation of two leading technologies such as Ad-hock and Centralized networking. This is worth notable paradigm shift, D2D Communication operating in Ad-hock network mode benefit the Mobile Operators. This approach would bring D2D Communication working with major technologies like cooperative communication, cognitive radio, Internet of Things (IoT). This methodology causes the network operators to improve the spectal effectiveness. At the same time, with centralized networking, D2D paradigm helps in enhancing the performance of the network, without losing control from the network operator.

Security requirements vary depending upon the use cases. As discussed earlier, typical D2D communication can fall under any one of these categories, such as full coverage, partial or out of coverage. As discussed earlier, typical UE's will have two radio links, one will be used for cellular communication and second link will be used for D2D communication.

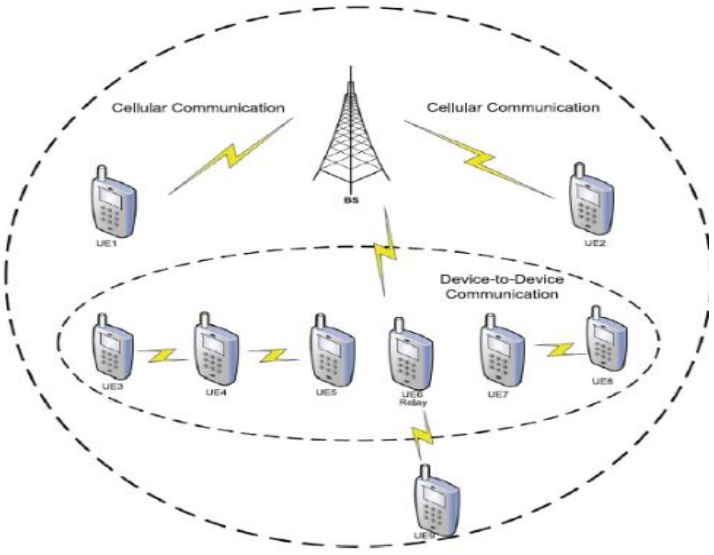

Figure 3. Cellular Communication and D2D Communication [15]

III. LIGHTWEIGHT CRYPTOGRAPHY

Ongoing research in the field of LightWeight Cryptography (LWC) indicates that it plays significant role in offering security for communication systems that lack computing power, as in case of IoT and Wireless Sensor Networks (WSN). LWC involves cryptographic algorithms aimed at resource-constrained devices. Sometimes this notion also conveys entirely different message that, it is meant for systems with lesser security demands, which is a myth, it is required for systems with higher security demands.

In comprehensive study of hardware implementation of some block ciphers which falls under the category of lightweight cryptography, such as SIMON, SPECK, PRESENT, KHUDRA and AES is carried out. This work covers mostly performance parameters such as throughput and power consumption of end devices. Also, security against cryptanalysis and side-channel security is discussed in detail. Essence of this work is different crypto-algorithms have different overheads with respect to counter measures used to defend against side-channel and cryptanalysis attacks. This work targets resource-constraints application, hence, can be applied for securing D2D communication. As we know Lightweight cryptography covers wide spectrum in terms of target devices and applications. Lightweight cryptography can be applied on devices with low hardware and memory capacity. Conventional cryptography can be applied on powerful computers, servers and smart phones. To identify the security requirements of resource constrained devices, Profile development is an important task, which is based on series of questions that needs to be answered. This will serve as a starting point for understanding of applications, identifying key bottlenecks if any, and helps in identifying additional constrains which may not be apparent at this point of time. Using lightweight design options such as Smaller Block Sizes, Smaller Key Sizes, Simpler Rounds, Lightweight Message

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

Authentication Codes, the performance advantages of lightweight block ciphers over standard block ciphers are accomplished.

As discussed in, the stringent safety requirements and resource constraints can be managed by using smaller block size, smaller key lengths, selecting lowcost implementation with efficient components such as datadependent bit permutations and using operations that enable implementation trade-offs balancing resource available on the target platform.

As mentioned in crypto-enabled and resource-restricted systems are in demand. This demand generates requirements for new algorithms and methods for cryptanalysis. Efficiency of Hardwarebased LWCalgorithms measured based on the amount of logic gates used. On an average this count will be up to up to 3000 logic gates per implementation. The efficiency of LWC hardware applications is comparable to traditional cryptographic methods viz. complexity of design, power and energy usage and throughput. LWC uses minimum quantity of hardware resources to accomplish the necessary functionality. Software implementation of LWC algorithms consumes less CPU cycles to minimize power consumption.

As discussed in Elliptic Curve Cryptography (ECC) is being considered for providing security to hand-held and mobile devices. ECC implementations uses shorter key length, also provides higher security on par with security provided by Rivest-Shamir-Adleman (RSA) implementation. This advantage of ECC over RSA turns out to be very appealing for mobile hand-held devices. ECC can also be used for securing D2D communication.

authors have analyzed multiple Lightweight cryptographic implementations. Comparing Security provided by Elliptic Curve Cryptography with that of RSA. Elliptic Curve Cryptography scores better for resource constrained devices because of its smaller operand lengths and relatively lower computational requirements.

authors presented advantages of Elliptic Curve Cryptography in terms of efficient key exchange between the communication end points. Elliptic Curve Cryptography also can be used authenticating the communication end points in terms of digital signature. the requirement is to choose the right Elliptic Curve to provide better performance and desired level of security based on the mobile and hand-held device requirements. This work can be extended by choosing right curves for different Voice Over Internet Protocol (VOIP) end points and analyzing the performance. This shows that Elliptic Curve Cryptography can also be used in D2D communication. Such an approach would be considered as good as applying lightweight cryptography.

IV. SECURITY IN D2D COMMUNICATION

Existing surveys on Securing D2D communication focused on applying Mobile Ad-hock Network security techniques. There are similarities between D2D communication in out of coverage scenario and MANET, at the same time D2D communication co-exist with cellular communication in terms of full coverage and partial coverage scenarios. Security is very important in D2D Communication. Common Security requirements of any wireless communication includes but not limited to Authentication, Data Confidentiality, Data Integrity, Privacy, Non-repudiation, Privacy, Availability, Access Control. As we know, by nature Wireless communication is prone to different types of attacks. Author's [32] have discussed different attack scenarios which are shown in Fig. 4. Attacks can be classified into Eavesdropping attack, Impersonation attack, Message modification attack, Man-in-the-middle (MITM) attack and Denial of Service (DOS) attack.

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

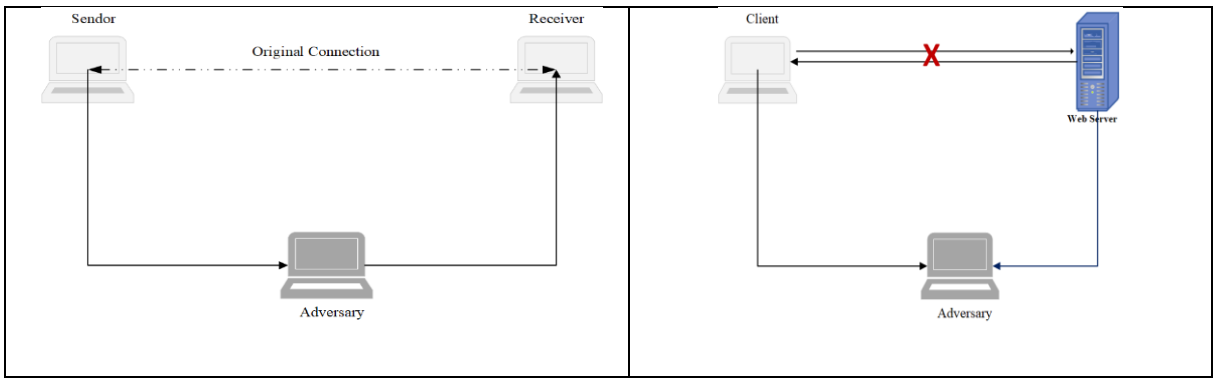

Figure. 4 Eavesdropping and MITM attack

Eavesdropping or passive listening attack can be launched by running a sniffing software. All unencrypted data can be sniffed by an adversary. Impersonating attack can be launched by spoofing link layer and network layer address. In case of message modification attack, an advisory will sniff the traffic and modify the message by crafting packets and injecting them into the network. Man-in-the-middle or MITM is a well know attack in the wireless network where an advisory establishes independent connections with sender and receiver. After establishing such connections, the attacker will modify the original communication between sender and receiver. One possible defense against such attack is to implement mutual authentication of sender and receiver.

Denial of Service (DOS) attack can be severe, where an attacker consumes all the resources for example, establishes the maximum number TCP connection with the target web server so that after reaching the limit web server will deny connections even to the legitimate users. Another type of DOS attack is reflection attack, where the attacker sends requests on behalf of victim machine to several servers on the Internet. When all these servers respond back with the victims IP as the destination, victim machine cannot handle this much traffic, could result in a crash.

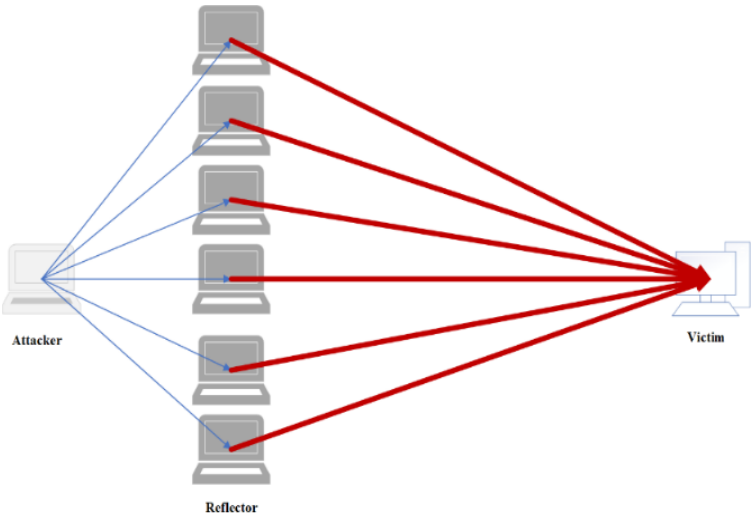

Figure.5 Denial of Service (DOS) attack

parameters used were UE latency and average relevant throughput. PKI based techniques used for providing the security, traffic offloading are the typical application scenario. The novel approach of gaming theory for clusterisation is used for creating clusters. This work mainly focuses on Group communication. Simulation results show that exploiting D2D connections lead to an increased throughput for the users at the cost of an additional delay and energy consumption due to the signaling message exchange locally in the cluster. Even though it covers all 3 scenarios, the LWC approach is not considered.

authors adopted social-aware strategy to optimize D2D communication by exploiting the social network layer and the physical wireless

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

network layer. Although this work focuses on content sharing based on Indian Buffet Process. Simulation findings shows improved system data rate. However, only privacy issue was addressed by providing an incentive for the users to share the content. The authors claim that, proposed system closely resembles the real life scenario. Proposed system considers in-band D2D communication, where most of the security issues will be handled by the Service Provider. However, there is a need to consider D2D outband communication scenarios. LWC techniques were not given consideration.

focused on out-of-coverage scenario, wherein UEs form D2D network without coming under any supervision of LTE infrastructure. Public Safety is the application scenario, based on probabilistic key Management scheme. The idea of random key pre-distribution among UEs from sensor networks was borrowed in this work, also used LWC technique such as a lightweight key exchange mechanism in D2D network formation. Simulation results (network connectivity analysis) of proposed secure protocol shows that the existence of trade-off points between connectivity and the increased overhead added by security for different values of the system parameter values. However, this work focused only on a subset of a bigger problem. Another limitation is only simulation of the proposed system is done, actual implementation was not done.

authors focus on extending PKI to partial coverage scenarios when Infrastructure becomes unavailable. This work is more related to group communication and handles the scenario of admission of new UE into the group. When infrastructure is not available UEs uses D2D link for communication otherwise LTE link will be used. Remarkable contribution of this work is security algorithm. This novel algorithm enables cellular network to manage and control group of devices involved in D2D communication. However, the suggested algorithm is neither implemented nor simulated.

authors target secure key exchange in D2D scenario. In this work authors have considered only D2D communication out-of-coverage scenario. Focus area of this work is Authentication and Key agreement. As we know Diffie-Hellman key exchange is vulnerable to MITM attack. In this work authors have implemented a secure key exchange scheme by integrating this into an existing Wi-Fi Direct protocol.

authors have not covered typical D2D scenarios like partial covered or full coverage scenarios, however focus is on ad-hoc mode, this work is mainly on mobile multiloop network, which is similar to D2D communication in out-of-coverage scenario. One main difference here is D2D communication could be one-hop communication whereas mobile communication in ad-hoc mode may involve multi-hop communication. However, Device-to-specific device in a group and Device-to-group communication were discussed by authors in this work. Ciphertext-PolicyAttribute-Based Encryption (CP-ABE)and protocol for Blue tooth authentication have been implemented. This research has taken possibly MITM attacks, replay attacks and collusion attacks as security requirements and communication costs, cost of storage and cost of computing as the parameter for measuring their implementation efficiency. Results indicate that the time taken to encrypt increases with the amount of attributes used in CP-ABE encryption, time taken to encrypt increases with amount of attributes used in CP-ABE encryption. However, the time needed to decrypt depends not on the number of attributes, but on the complexity of the access policy.

In this work authors proposed a scheme based on the Blue tooth protocol, which resolve the initial key establishment and integrity

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

problems in the presence of internal adversaries in a multi-hop networks and can be expanded to other D2D protocols such as Wi-Fi Direct. As per the analysis CP-ABE is comparatively expensive, because CP-ABE is done once during the initial authentication operation for secure PIN delivery, which covers only authentication part of the security requirement, However, there is a need for securing the the data in transit. LWC techniques can be leveraged for achieving this objective. Simulation is not done, Implementation of the initial key establishment protocol on an Android smartphone is done using Java and the CP-ABE open source library.

authors have taken D2D network layer such as impact of Denial of Service (DoS). Experimental results shows that DoS attacks can force UEs to lose the Wi-Fi connection, which goes undetected by the access point(AP) or the cellular network. This work includes situations of in-coverage and ad-hoc communication mode. However, the scope of this work is limited, concentrating only on one attack and ignoring other elements. However, in this case LWC technique were not considered.

A lightweight on-demand-puzzled Identity Based Encryption(IBE) solution for secure D2D discovery and communication was introduced in[10]. The authors developed a protocol based on the altered IBE scheme to provide D2D customers with assistance for privacy and legal interception. This protocol is validated in a social network scenario for D2D communication. Security analysis of this protocol is carried out for both single and multiple domain use cases. This work is related to addressing security issues in discovery and communication phases, Scenarios covered are full coverage and UEs exist in single domain and full coverage but UEs in different domains Authors proposed hybrid solution that integrates IBE and ECC. Focus is key management in the scenarios where UEs belong to same operator and another scenario where UEs belong to different operators.

Authors considered only full coverage scenario of D2D communication, related physical layer security. A novel approach has been proposed wherein D2D interference used to enhance security and also create extra transmission opportunities for the D2D users. This model uses stochastic geometry for D2D resource allocation. The limitation of the proposed model is the communication mode of each user such as , cellular mode or D2D mode is preset cannot be changed, but in practice this is not true, every user can change communication mode. The suggested model can withstand the attack by Eavesdropping, but it is possible to mount other attacks. This work does not explore LWC methods.

Authors proposed Security framework for proximity services, this work covers all 3 scenarios of D2D communication. Application scenario is extending the coverage and they have used game theory centric based clustering approach. Implementation is done using OpenSSL with RSA algorithm. Security system they have proposed is based on PKI technique and simulated their work using MATLAB. Experimental result shows that there is some amount of signaling overhead, but connectivity was provided, and performance parameters were good. In this work lightweight cryptographic techniques were not used.

Authors had investigated access control for D2D communication underlaying cellular network. The network Calculus theory is being used and proposed model facilitates interference avoidance between D2D and Cellular communication. Proposed system employs multi-priority model which assigns strictly highest priority for cellular users and multiple levels of priority for D2D users in a single cell. Numerical simulation of proposed system shows that Quality of Service (QoS) of cellular system enhanced,

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

however, low priority D2D user's communication is impacted not only by the cellular users, but also by higher priority D2D users. Access control is one of the security requirements, but at the same time other security requirements like authentication, authorization, data confidentiality, data integrity could have been considered. LWC technique plays a very important role, which is not considered in this work.

authors proposed a scheme based on secure group key agreement and routing. This work is related to authentication based on Public Key Infrastructure (PKI). Simulation results shows that the suggested algorithm can be applied to D2D out-of-coverage network scenario up to 64 Ad-hoc nodes. This work does not cover LWC techniques.

Authors have done extensive survey of Security in D2D communications. The entire work is based on classification of D2D communication in layered approach. D2D communication security requirements have been identified for each layer namely, Application layer, Network layer, Media Access layer and Physical layer. Contribution of existing work in this area by various researchers is mapped to these security requirements at each layer is compared against few identified parameters, operational mode (Network assisted mode, Adhoc mode), purpose, scenario and applications. This work provides guidelines for the future research. However, lightweight cryptographic techniques were not considered while comparing the existing work.

Authors' work includes the full coverage scenario, 3 protocols have been suggested for UE's authentication. The Use case scenario is Traffic offloading and Social Networking. The traffic offloading scenario network detects that 2 UE's are connected to the same eNodeB, the application does not require a D2D link, but this scenario is used by the network to reduce the access and core network load by ensuring the D2D connection used for this scenario. However, in the Social Networking scenario, applications in each device require a D2D link between them, social networking application in UE1 discovers the target UE is in proximity, after such discovery D2D link between these 2 UEs is established. All 3 protocols proposed two types of channel are used for processing the key exchange. Public wireless channel which is an insecure channel through which public keys are exchanged, even advisory can get the public keys, susceptible to MITM attack, Encrypted Dedicated channel similar to public channel but data is encrypted before sending through this channel, adversaries will not have access. Simulation is done using MATLAB results are compared with existing two protocols SeDS: Secure Data sharing Strategy and SeCD. Simulation results show that communication overhead increases in protocol-3 due to the dependency of eNodeB which generates and compares Keys. However, this work does not focus on the use of lightweight cryptographic techniques, also does not cover partial coverage and no coverage scenarios.

Authors suggested Security Scoring (SeS), which is computed using legitimacy patterns. Scores obtained from static and random allocation of legitimacy patterns are compared. Simulation results shows that for detection, shorter legitimacy pattern is sufficient when attack is being carried out for longer duration. Attacks are being carried out with the combination of encryption, authentication, secure routing and forwarding and prevention of virus, worms and malicious code. SeS method uses LWC techniques. SeShelps detecting attacks at physical layer with lessor computational efforts. Additionally, implementing security at physical layer will complement security of higher layers.

Authors have considered physical layer security, wherein radio resource allocation is

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

formulated as a matching problem in a weighted bipartite graph. Simulation results indicate that system secrecy capacity improved by introducing D2D communications underlaying cellular networks. However, LWC techniques are not considered.

In [26] authors considered physical layer security provided by a direct D2D connection between two nodes. Simulation results indicates that D2D mode offers better security compared to decode-and-forward approach involving Access Point. However, LWC is not considered in this work.

authors have proposed secure message delivery protocol to securely deliver message for multi-hop D2D communication. In this work D2D communication full coverage and D2D communication partial coverage scenarios are not covered, only out of coverage scenario is covered. However, in this work, authors have not considered applying lightweight cryptographic techniques for providing security for D2D communication.

authors have proposed crypto system based on Elliptic curve and ElGamal over public-key infrastructure (EEoP). EEoP uses ECC for creation of keys and uses ElGamal for encryption and decryption over public-key infrastructure. The proposed system can be used in partial coverage scenario of D2D communication, also computationally lightweight. EEoP ensures the confidentiality and integrity of the communication.

authors have proposed a fast secret key extraction (KEEP) protocol to establish secure secret key between two communication entities. KEEP uses a recombination validation mechanism to obtain coherent secret keys from Channel State Information (CSI) measurements of all Orthogonal Frequency Division Multiplexing (OFDM) sub carriers. It achieves a high key security level and a fast key generation rate. Results of simulation show that KEEP achieves a high level of security against different attacks such as eavesdropping and predictable channel attack. However, this work considers only full coverage scenario of D2D communication.However, LWC is not considered in this work.

authors have taken Wi-Fi Direct as the promising protocol for offering security in D2D communication. In this work authentication-string-based key agreement protocol been proposed and integrated into the current Wi-Fi Direct protocol. Proposed protocol has been implemented on Android smart phones. However, this is not a complete solution. To create and sustain a secure connection, Wi-Fi Direct utilizes the WPA security and certification protocols. Through Wi-Fi Direct, sensitive activated devices such as printers, attackers can access the Wi-Fi network and WLAN. To persuade an activated device to route from Wi-Fi to a local area network, Attackers can use the link via Wi-Fi Direct. Therefore, use of lLWC methods is available.

authors have presented a benchmarking framework for evaluating lightweight block ciphers which are widely used micro controller platforms for IoT devices. However same thing can also be used for benchmarking lightweight block ciphers for D2D communication. This framework consists of metrics of interest such as Execution time, RAM footprint and Binary code size. We are hoping to use these metrics in our next work, while implementing lightweight block ciphers for securing D2D communication.

V. CONCLUSION

D2D communication is going to play very important role in near future. D2D communication can help in various scenarios like disaster recovery, emergency services. D2D communication is getting lot of attention 3GPP

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

has already proposed proximity service which will be part of LTE-A.

Security is very important, however due to the very nature of D2D communication end devices need to communicate securely without using the infrastructure. Conventional cryptography might be good but not suitable for D2D communication. In such scenario's lightweight cryptography can be a good choice. In this paper we have analyzed current work on securing D2D communication. Most of the literature on D2D security confined to authentication of end user or devices. However, there is a need for providing security for data in transit. There are many open issues which can be investigated further, also there is huge scope for adopting lightweight cryptographic techniques which eventually enhance security and performance.

VI. ACKNOWLEDGEMENTS

This is a survey work related to my research domain. I would like to thank VTU Regional Research Center(RRC) Belagavi, Principal and Management of Cambridge Institute of Technology K.R Puram, Bangalore.

VII. APPENDIX

In this appendix, we provide comparison of current research work related to Securing D2D communication with application scenario, security considerations and use of lightweight cryptographic techniques.

APPENDIX
Comparative Analysis of Secure D2D Communication

Reference	D2D Full Coverage	D2D Partial Coverage	D2D Out of Coverage	Application Scenario	Security Considerations	Lightweight Cryptographic Techniques
[3]	Yes	Yes	Yes	GORUP communication	Privacy	No
[4]	No	No	No	Social networking Media sharing (traffic offload)	Privacy	No
[5]	No	No	Yes	Public safety	Secrecy	Yes
[6]	Yes	Yes	Yes	Admission of new users into the group, PKI based secure group construction	Admission control	No
[7]	No	No	Yes	Diffie-Hellman based key agreement	Secrecy	Yes
[8]	No	No	No	Multihop Communication in Adhoc mode,	Authentication	No

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

				Cipher text Policy-Attribute Based Encryption		
[9]	Yes	No	No	Impacts of Denial-of-Service (DoS) attacks in a D2D underlaying network	Availability	Yes
[10]	Yes	No	No	UE's exists in single domain, ECC and Identity Based Encryption Techniques	Privacy	Yes
[11]	Yes	No	No	Physical layer security, using interference exploitation techniques in D2D-enabled cellular networks,	Eavesdropping	No
[12]	Yes	Yes	Yes	OpenSSL with RSA, extending the coverage using Game theory-based Clustering approach	Secrecy	No
[13]	No	No	No	Multi priority model, Network Calculus theory	None	No
[14]	Yes	Yes	Yes	PKI based Group Key Agreement and routing, offload local traffic	Authentication	No
[19]	Yes	No	No	Man-in-the-Middle attack, Secure Key Exchange Traffic Offload, Social Networking	Authentication	No

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

[20]	No	No	No	Continuous authenticity using Security-scoring using legitimacy pattern	Authentication	Yes
[25]	No	No	No	System secrecy capacity	Secrecy	No
[26]	No	No	No	Security provided at Physical layer	Eavesdrop	No
[27]	No	No	Yes	Secure path to deliver the message	Secrecy	No
[30]	No	Yes	No	Man-in-the-Middle attack, Secure Key Exchange	Secrecy, Integrity	Yes
[31]	Yes	No	No	Secure Key Exchange	Eavesdropping, Secrecy	No
[32]	Yes	Yes	Yes	Secure Key Exchange	Secrecy	No

VIII. REFERENCES

[1] A. Asadi, Q. Wang and V. Mancuso., "A Survey on Device-to-Device Communication in Cellular Networks," IEEE CommunicationsSurveys & Tutorials, vol. 16, pp. 1801-1819, 2014.

[2] Pimmy Gandotra, Rakesh Kumar Jha and Sanjeev Jain, "A Survey on Device-to-Device (D2D) Communication: Architecture and Se-curity Issues," Journal of Network and Computer Applications, vol. 78, pp. 9-29, 2017.

[3] A. Orsino and A. Ometov, "Validating Information Security Framework for Offloading from LTE onto D2D Links," in Pro-ceedings of the 18th Conference of Open Innovation and Seminar on Information Technology (FRUCT-ISPIT), pp. 241-247, 2016.

[4] Y. Zhang, E. Pan, L. Song, W. Saad, and Z. Dawy, "Social Network Aware Device-to-Device Communication in Wireless Networks," in IEEE Transactions on Wireless Communications, vol. 14, No.1, pp.177-190, 2015.

[5] L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," International Symposium on Wireless Communications Systems (ISWCS), pp. 548-552, 2014.

[6] Aleksandr Ometov,Konstantin Zhidanov,Sergey Bezzateev,Roman Florea,Sergey Andreev and Yevgeni Koucheryavy, "Securing Network-Assisted Direct Communication: The Case of Unreliable Cellular Connectivity," in Proceedings of IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 826-833, 2015.

[7] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila and Y. Cheng, "Secure key establishment for Device-to-Device communications," IEEE Global Communications Conference,(GLOBECOM), pp. 336-340, 2014.

[8] Kwon, H., Kim, D., Hahn, C. et al, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks", Multimedia Tools and Applications, vol. 76, Issue 19, pp.19507–19521, 2017.

[9] A. Hadiks, Y. Chen, F. Li and B. Liu, "A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks," in IEEE 11th

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

Consumer Communications and Networking Conference (CCNC), pp. 507-508, 2014.

[10] E. Abd-Elrahman, H. Ibn-khedher, H. Afifi and T. Toukabri, "Fast group discovery and non-repudiation in D2D communications using IBE", International Wireless Communications and Mobile Computing Conference(IWCMC), pp.616-621, 2015.

[11] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui and X. Wang, "Interference Exploitation in D2D-Enabled Cellular Networks: A Secrecy Perspective", in IEEE Transactions on Communications, vol. 63, No. 1, pp. 229-242, 2015.

[12] A. Ometov, A. Orsino, L. Militano, G. Araniti, D. Moltchanov and S. Andreev, "A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity," Computer Networks, vol. 107, Part 2, pp. 327-338, 2016.

[13] Huang, Jun, Yi Sun, Zi Xiong, Qiang Duan, Yanxiao Zhao, Xianghui Cao, and Wei Wang, "Modeling and Analysis on Access Control for Device-to-Device Communications in Cellular Network: A Network-Calculus-Based Approach," in IEEE Transactions on Vehicular Technology, vol. 65, No. 3, pp. 1615-1626, 2016.

[14] Younchan Jung, Enrique Festijo, Marnel Peradilla, "Joint operation of routing control and group key management for 5G ad hoc D2D networks" International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1-8, 2014.

[15] Udit Narayana Kar and Debarshi Kumar Sanyal, "An Overview of Device-to-device Communication in Cellular Networks", ICT Express, vol 4, issue 4, pp. 203-208, 2018.

[16] Kerry A. McKay, Larry Bassham, Meltem Sönmez Turan, Nicky Mouha, "Report on Lightweight Cryptography", National Institute of Standards and Technology Internal Report 8114, 2017.

[17] Sadhukhan, R., Patranabis, S., Ghoshal, A. et al.,"An Evaluation of Lightweight Block Ciphers for Resource-Constrained Applications: Area, Performance, and Security", Journal of Hardware and Systems Security, vol 1, issue 3, pp. 203–218, 2017.

[18] Othmane Nait Hamoud, Tayeb Kenaza and Yacine Challal, "Security in device-to-device communications: a survey," in IET Networks, vol. 7, no. 1, pp. 14-22, 2018.

[19] R. Sedidi and A. Kumar, "Key exchange protocols for secure Device-to-Device (D2D) communication in 5G," 2016 Wireless Days (WD), pp. 1-6, 2016.

[20] Abualhaol and S. Muegge, "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns," 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5763-5771, 2016.

[21] Panasenko, Sergey P. and Sergey A. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches", International Journal of Computer Theory and Engineering, vol. 3, No. 4, pp. 516-520, 2011.

[22] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. et al.,"A review of lightweight block ciphers", Journal of Cryptographic Engineering, vol. 8, issue 2, pp. 141–184, 2018.

[23] Ajithkumar V and K Satyanarayan Reddy, "A Survey on Security of Mobile Handheld devices through Elliptic Curve Cryptography", ACCENTS Transactions on Information Security, vol.2, no.6, pp.32-35, 2017.

[24] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," in IEEE Design & Test of Computers, vol. 24, no. 6, pp. 522-533, 2007.

[25] H. Zhang, T. Wang, L. Song and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," 2014 IEEE International Conference on Communications (ICC), pp. 2319-2324, 2014.

[26] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu and C. Zhao, "Device-to-device communications: The physical layer security advantage," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1606-1610, 2014.

[27] Panaousis E., Alpcan T., Fereidooni H., Conti M. "Secure Message Delivery Games for Device-to-Device Communications," Decision and Game Theory for Security. GameSec 2014. Lecture Notes in Computer Science, vol.8840, pp. 195-215., 2014.

[28] Ajithkumar Vyasarao and K Satyanarayan Reddy, "Application of Elliptic Curve Cryptography for Mobile and Handheld devices", in Proceedings of International Conference on Contemporary Issues of Science, Engineering and Management (ICCI-SEM-2K17), pp. 87-91, 2017.

[29] Dinu, D., Corre, Y.L., Khovratovich, D. et al., "Triathlon of light-weight block ciphers for the

January - February 2020
ISSN: 0193 - 4120 Page No. 5419 - 5432

Internet of things", Journal of Cryptographic Engineering, pp.1-20, 2018.

[30] Yasir Javed, Adnan Shahid Khan, Abdul Qaharand Johari Abdullah, "EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks", Journal of Telecommunication Electronic and Computer Engineering, vol. 9, no. 3-11, pp 99-105, 2018.

[31] M. Janardhana Raju Raju, Dr. P.Subbaiah, V.Ramesh, "A Novel Elliptic Curve Cryptography Based AODV for Mobile Ad-Hoc Networks for Enhanced Security", Journal of Theoretical and Applied Information Technology, vol.58, issue 3, 2013.

[32] Wei Xi et al., "KEEP: Fast secret key extraction protocol for D2D communication," 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), pp. 350-359, 2014.

[33] W. Shen, B. Yin, X. Cao, L. X. Cai and Y. Cheng, "Secure device-to-device communications over WiFi direct," in IEEE Network, vol. 30, no. 5, pp. 4-9, 2016.

[34] Noura, Mahda & Nordin, Rosdiadee., "A Survey on Interference Management for Device-to-Device (D2D) Communication and its Challenges in 5G Networks", Journal of Network and Computer Applications, vol 71, pp. 130-150, 2016.

[35] B. Cho, K. Koufos, R. Jäntti, Z. Li and M. A. Uusitalo, "Spectrum allocation for multi-operator device-to-device communication," 2015 IEEE International Conference on Communications (ICC), pp. 5454-5459, 2015.

[36] Y. Zhao and W. Song, "Survey on Social-Aware Data Dissemination Over Mobile Wireless Networks," in IEEE Access, vol. 5, pp. 6049-6059, 2017.

[37] Melki, Reem & Noura, Hassan & Mansour, Mohammad & Chehab, Ali, "A survey on OFDM physical layer security", Journal of Physical Communication, vol. 32, pp. 1-30, 2019.

[38] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally and M. A. Javed, "A Survey of Device-to-Device Communications: Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2133-2168, 2018.

BIOGRAPHIES OF AUTHORS

	Ajith Kumar. V is currently a Ph.D. student at Visvesvaraya Technological University, Regional Research Center of Belagavi. His research focus is on security for resource-constrained devices and application of lightweight cryptographic techniques for securing D2D communication. He obtained B.Sc. degree from University of Mysore in 1991 and his M.C.A., degree from Kuvempu University in 1999. His interest includes Computer Forensics, Cyber Secu-rity. He is life member of Cryptology Research Society of India (CRSI).
	K. Satyanarayan Reddy. His qualification includes Ph.D. in Computer Science (Dravidian University, Kuppam, AP), MTech in Computer Applications (Dept. Of CSE, ISM Dhanbad). He has worked as faculty in many Engineering Colleges ,currently he is associated with Dept. of CSE, Cambridge Institute of Technology, Bangalore. He has more than 25 Re-search Papers (National and International) in his credit and has chaired national and international conferences. Delivered Keynote address in few national level conferences.